

T-110.4100

Tietokoneverkot

17.1.2012

Miika Komu

Alkup. kalvot: Sanna Suoranta

Tietoliikenneohjelmistot

Tietotekniikan laitos

Aalto-yliopisto

Kurssin sisältö

- TCP/IP-verkot ja niiden toiminta
- Verkkosovellusten suunnittelu ja ohjelmointi

Tietoa tästä kurssista

- <https://noppa.aalto.fi/noppa/kurssi/t-110.4100/>
- IRC: #verkot
- <https://piazza.com/>
 - Tarkemmat tiedot Nopassa etusivulla
- T-110.4100@tkk.fi (henkilökohtaiset kysymykset)
- <http://cse.aalto.fi/fi/opinnot/paaaineet/tietoliikenne/ohjelmistot-a2/>

Esitiedot

- T-110.2100 Johdatus tietoliikenteeseen ja T-106.3101 Ohjelmoinnin jatkokurssi T2
- Eli oikeastaan
 - Tiedonsiirron perusteet
 - Tietotekniikan perusopintojen ohjelmointikurssit, erityisesti C-kieli

Ilmoittautuminen

- Ilmoittautuminen on avattu WebOodiin
 - Ilmoittautuminen päättyy 30.1.2012
- Tentteihin tulee ilmoittautua erikseen viimeistään viikkoa ennen tenttiä
 - Kumpaankin osatenttiin erikseen
 - Ilmoittautuminen on avattu kaikkiin tentteihin
 - Muistakaa perua ilmoittautuminen, jos ette tule! (oodissa tai sähköpostitse)

Kurssin osasuoritukset ja arvostelu

- Pakolliset
 - Osatentti 1: perus-TCP/IP. 33% loppuarvosanasta
 - Osatentti 2: ohjelmointi, NAT, verkonhallinta jne. 33% loppuarvosanasta
 - Harjoitustyö 34% loppuarvosanasta
 - Palaute on pakollinen!
- Vapaaehtoiset mutta hyödylliset 😊
 - Luennot+muistiinpanot
 - Kirjan lukeminen, jne

Luennot ja harjoitukset

- Uutta: kurssi luennoidaan sekä III että IV periodeilla
 - Tiistaisin 10-12 salissa T2
- Assareilla ei erillistä vastaanottoa, mutta apua saatavissa pyydettäessä
 - Mahdollisesti otetaan varausjärjestelmä käyttöön
- Tarkempi aikataulu löytyy kurssin [www-sivuilta](https://noppa.aalto.fi/noppa/kurssi/t-110.4100/) nopasta
 - <https://noppa.aalto.fi/noppa/kurssi/t-110.4100/>

Luennot

- | | | |
|------------|-------------------------|------------------------------|
| • Ti 17.1. | Johdanto + IPv4 | Miika Komu |
| • Ti 24.1. | IPv6 | Miika Komu |
| • Ti 31.1. | Verkko-ohjelmointi | Samuli Sorvakko ja assarit |
| • Ti 7.2. | Reititys 1 (IGP) | N.N. |
| • Ti 14.2. | Reititys 2 (EGP) | N.N. |
| • Ti 21.2. | Liikkuvuus | Matti Siekkinen |
| • Ti 28.2. | TCP & UDP | Matti Siekkinen |
| • Ti 13.3. | DNS & DNSsec | Bengt Sahlin |
| • Ti 20.3. | Harjoitustyö osat 2 & 3 | Assarit |
| • Ti 27.3. | Protokollasuunnittelu | Miika Komu |
| • Ti 3.4. | Ei luentoa | (Varalla) |
| • Ti 17.4. | Verkonhallinta | Jaakko Kotimäki |
| • Ti 24.4. | NAT | Ari Keränen |
| • Ti 8.5. | Uutuudet | Yrjö Raivio, Matti Siekkinen |

Oppimateriaali

- Douglas E. Comer, Internetworking with TCP/IP, Volume 1, Pearson Prentice Hall, 2006 tai joku muu perusoppikirja (Nopassa)
- Opetusmonisteita Nopassa
 - Luennoijien kirjoittamaa materiaalia
 - Linkkejä nettiin
- Kalvot lisätään kurssin luentoaikatauluun
 - Pääasiallisesti luennon tukimateriaali, ei oppimateriaali sellaisenaan
 - Älkää tulostako niitä Aallon tulostimille!

Tentit

- Tenttipäivät 7.3.2012 ja 16.5.2012 (ks. oodi!)
 - Tenttiin ilmoittauduttava viimeistään viikkoa ennen tenttiä
- Kaksi osatenttiä, kumpikin 33% arvosanasta
 - Molemmat suoritettava hyväksytysti kurssin läpäisemiseksi
 - Kumpikin osatentti arvostellaan asteikolla 0-5
 - Kaikkina tenttikertoina (tenttikausina) voi tehdä jommankumman osatentin (tai molemmat osatentit yhdellä kerralla)
 - Kumpaankin osatenttiin ilmoittaudutaan erikseen!
 - Vanhoja tenttejä kurssin Noppa- ja arkistosivuilla

Tentti (jatkuu..)

- Perukaa ilmoittautuminen, jos ette tule paikalle!
 - Oodissa, tai ilmon sulkeuduttua sähköpostitse
- “Opiskelijan tulee ilmoittautua kokeeseen viikkoa ennen koetilaisuuden järjestämistä, jollei opettaja hyväksy myöhempää ilmoittautumista. Ilmoittautuminen katsotaan kokeeseen osallistumiseksi, ellei sitä ole peruutettu ennen kokeen alkamista. **Kokeessa kolmasti hylätyn opiskelijan on neuvoteltava asianomaisen opettajan kanssa kurssin suorittamisesta.** ”
(*tutkintosäätö*)

Harjoitustyö

- Harjoitustöiden tehtävänanto julkaistaan kurssin noppasivuilla. Kolme osaa:
 - Socket-ohjelmointi tehtävä
 - DNS tehtävä
 - Tehtävä TCP/IP pinolla sulautetuille järjestelmille
- Palautus (koodi ja raportti) + demo
- Pisteytys (0 on hylätty):
 - Kierros 1 (0-3 p)
 - Kierros 2 (0-4 p)
 - Kierros 3 (0-3 p)
 - Pisteet lasketaan yhteen ja jaetaan kahdella
- Harjoitustyö tehdään yksin
 - C-kieli tarpeen! Laita mailia muusta kielestä

Kysyttävää järjestelyistä?

Jo osattavaa

Käyttäjän sovellukset:

- sähköposti (SMTP, POP, IMAP)
- WWW (HTTP)
- FTP,
- news (NNTP)
- P2P

tietoturvan
käsitteet

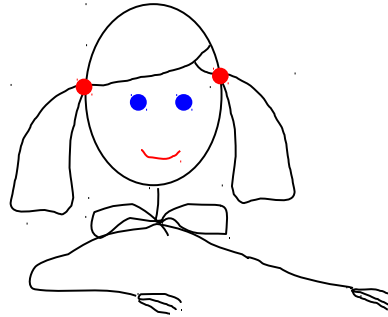
UDP, TCP
kuittaukset

IPv4

ARP

Ethernet

Aiheuttaa viiveitä,
häviöitä jne.
(out of scope)



Sovelluskerros

Kuljetuskerros

Verkkokerros

Linkkikerros

Fyysinen kerros

Tällä kurssilla

Infrastruktuuri-
palvelut: DNS,
SNMP, NAT

Tietoturvaratkaisut:
TLS, DNSsec

protokollasuunnittelu
verkko-ohjelmointi

Socket-rajapinta
ohjelmoinnille

TCP "kokonaan" eli
virhetilanteiden käsittely

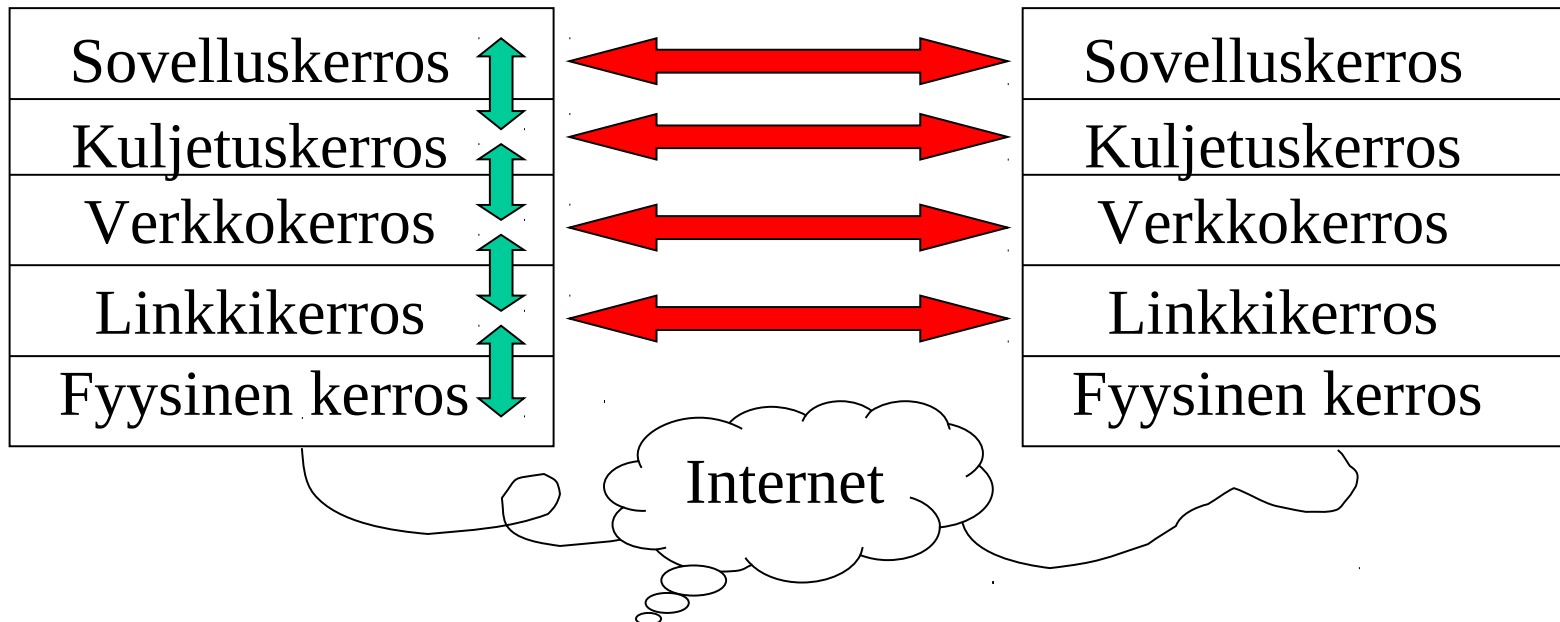
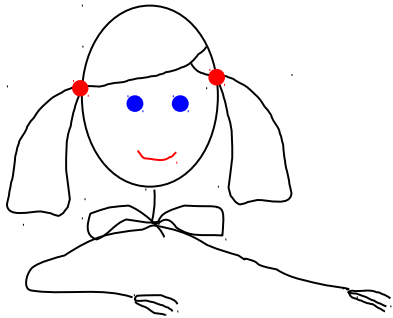
IPv6, reititysalgoritmit,
IPsec

Ethernet, miten IP-osoitetta
vastaava ethernet
osoite löydetään IPv6:ssa
(ja toistepäin)

Rajapinta ja protokolla

- mitä
tehdään samassa
koneessa esim.
kapsulointi

- koneiden välillä
- viestiformaatit
- osapuolten
"tunnistus"
- viestien käyttö



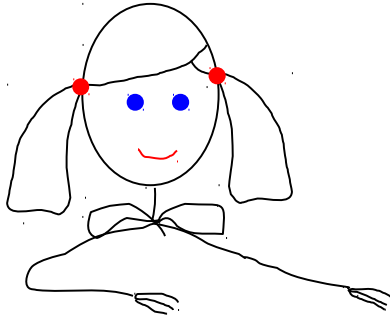
Internet-protokolla versio 4

Kertaus

luvut 4, 6 ja 8

Luennon sisältö

- IPv4 ominaisuudet ja tehtävä
- IPv4 otsake ja käyttö
- IPv4 osoitteet
 - Ali- ja yliverkotus
 - Muut ratkaisut: NAT ja DHCP
- ICMP
 - Virhetilanteiden käsittely



Internet-protokolla

SMTP	SIP	HTTP
SSH		IRC
TCP	UDP	SCTP
IP		
Ethernet	Token ring	
valokuitu	cat-5	

IP

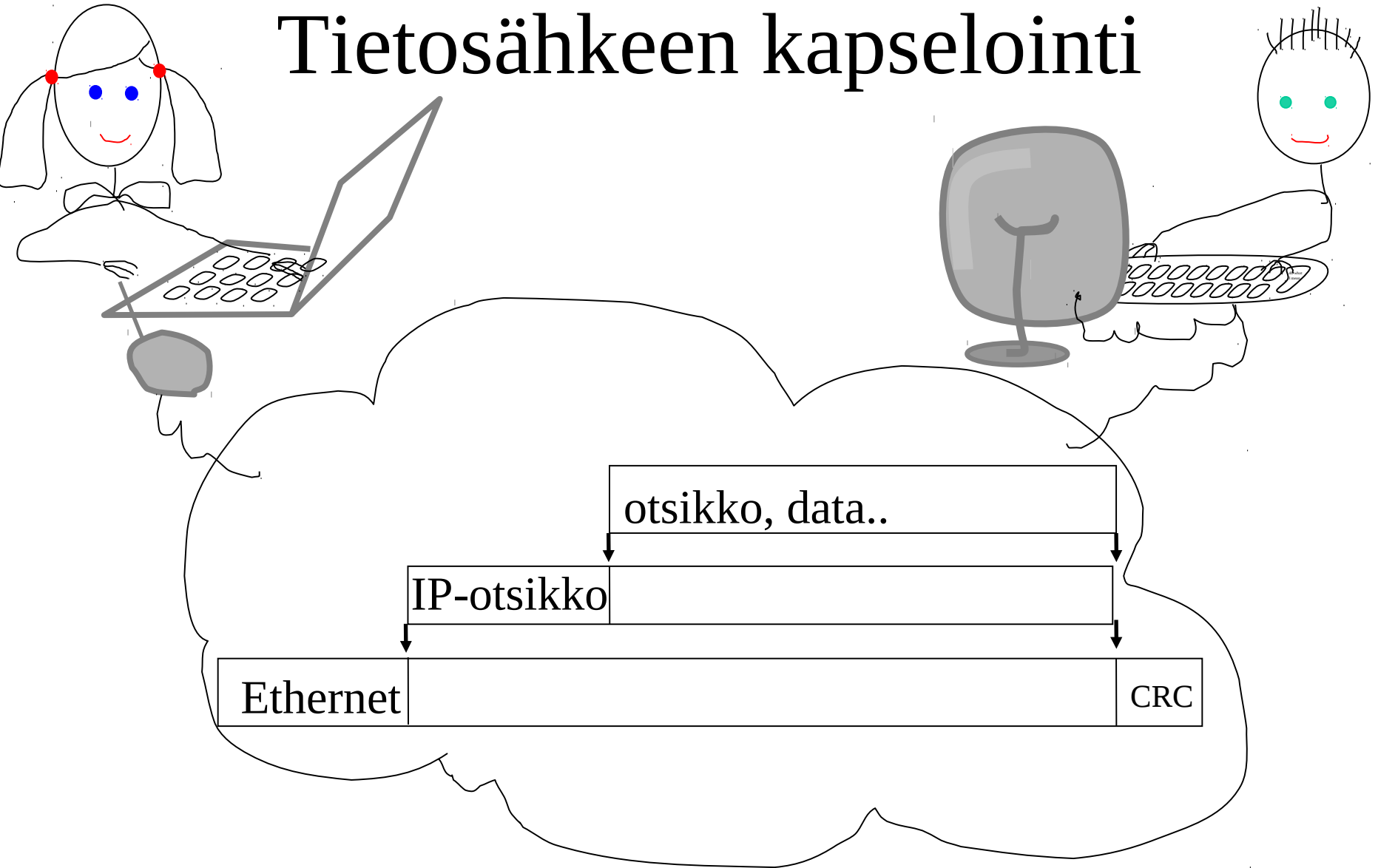
Internet-protokolla

- Internet-protokolla on yhdistävä tekijä kaikkien sovellusten ja kaikenlaisten verkko-tekniologioiden välissä

Internet-protokolla (IP)

- Pakettipohjainen (packet oriented)
 - viesti jaetaan paketteihin
- Yhteydetön (connectionless)
 - jokainen tietosähke (datagram) käsitellään itsenäisesti
- Epäluotettava (unreliable)
 - perillemeno ei taata
 - paketit voivat monistua, viivästyä, järjestys voi vaihtua...
- Päästä päähän (end-to-end)
 - lähettäjän ja vastaanottajan ei tarvitse olla samassa verkossa

Tietosähkeen kapselointi



IP-otsikon rakenne (RFC 791)

0	4	8	16	19	24	31
VERS	O.PIT	PALV.TYYPPI	KOKONAISPITUUS			
TUNNISTE			LIPUT	LOHKON SIJAINTI		
ELINIKÄ (TTL)		PROTOKOLLA	OTSIKON TARKISTUSSUMMA			
LÄHDEOSOITE						
KOHDEOSOITE						
OPTIOT (JOS ON)					TÄYTE	
data...						

IP-otsikon kentät

- VERSio numero = 4
- Otsikon pituus (O.PIT) 32 bitin sanoina
 - min 5 (5*32 bittiä) + optiot
 - kertoo siis lähinnä optioiden pituuden
- PALVELUN TYYPPI

0	6 7
CODEPOINT	00

 - palvelun laadun määrittely, esim DiffServ
 - alunperin toisella tavalla

IP-otsikon kentät

- KOKONAISPITUUS

- otsikko+data-osion pituus oktetteina

- LIPUT, kolme bittiä:

0	DF	MF
---	----	----

- DF: 0 = saa lohkoa, 1 = ei saa lohkoa

- MF: 0 = viimeinen lohko, 1 = lisää lohkoja

- LOHKON SIJAINTI + TUNNISTE

- kts. lohkominen

IP-otsikon kentät

- ELINIKÄ
 - maksimi”aika”, jonka paketti saa vaeltaa verkossa
 - alun perin sekunteja; nyt jokainen reititin vähentää vähintään yhdellä
- PROTOKOLLA
 - Ylemmän kerroksen protokolla, joka on data-osiossa
 - Esim ICMP=1, TCP = 6, UDP =17, IPv6=41

IP-otsikon kentät

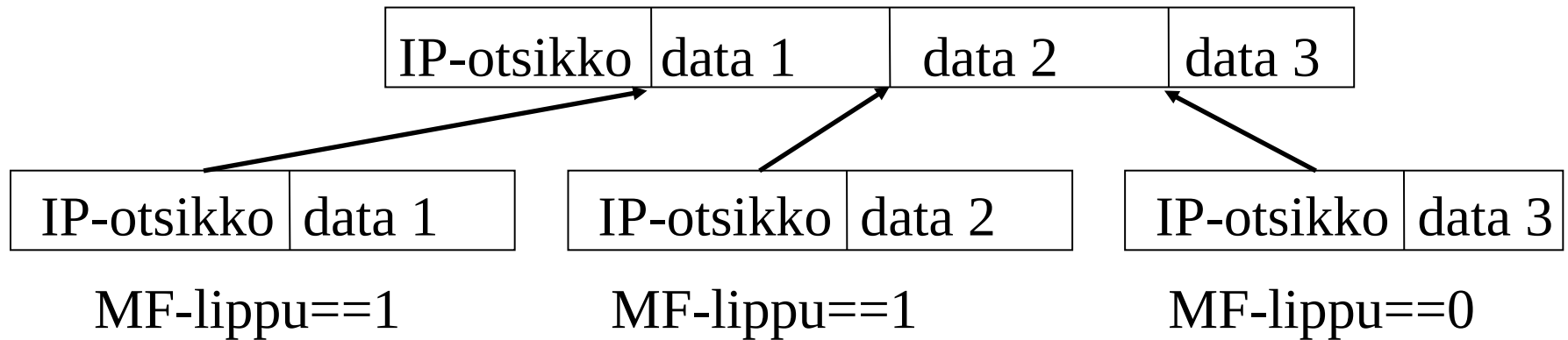
- TARKISTUSSUMMA
 - 16-bittinen yhden komplementtisarvon yhden komplementti otsikon kentistä
 - kertoo, onko otsikko ehjä
 - ylemmillä kerroksilla omat tarkistussummat
- LÄHDE- ja KOHDEOSOITTEET
 - 32-bittisiä, kts alla

Tietosähkeen lohkominen

(englanniksi datagram fragmentation)

- Tietosähke ei aina mahdu fyysisen verkon kehykseen, joten se pitää lohkoa useampaan palaan
 - tehotonta, joten yritetään välttää selvittämällä verkon enimmäispituus eli MTU (Maximum transfer unit)
- Tietosähke kootaan vasta vastaanottajalla
 - Odotetaan tietty aika, että kaikki lohkot tulisivat perille

Tietosähkeen lohkominen

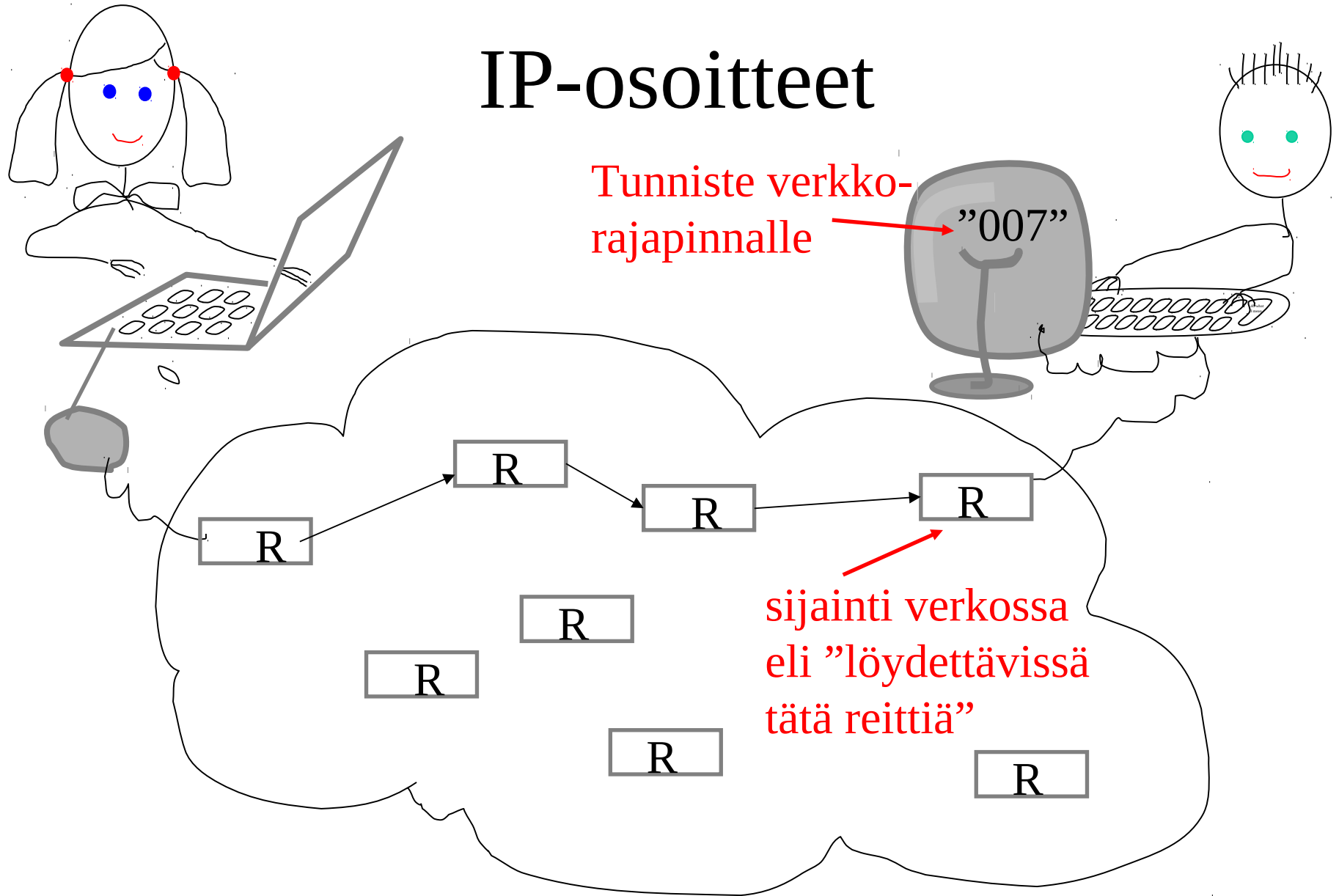


- Jokaisella tietosähkeellä on TUNNISTE, jonka avulla lohkot kootaan takaisin
- Lohkon sijainti: oktettia alkaen alkuperäisen datan alusta
- kokonaispituus: lohkotun sähkeen pituus

IP:n optiot

- Käytetään pääasiassa verkon testauksessa ja vianmäärityksessä (jos siinäkään)
- Ohjeellinen ja täsmällinen lähdereititys, reitin seuranta, jne

IP-osoitteet



IPv4-osoitteet (RFC 796, 1981)

- Alkuperäinen luokallinen osoitteistus

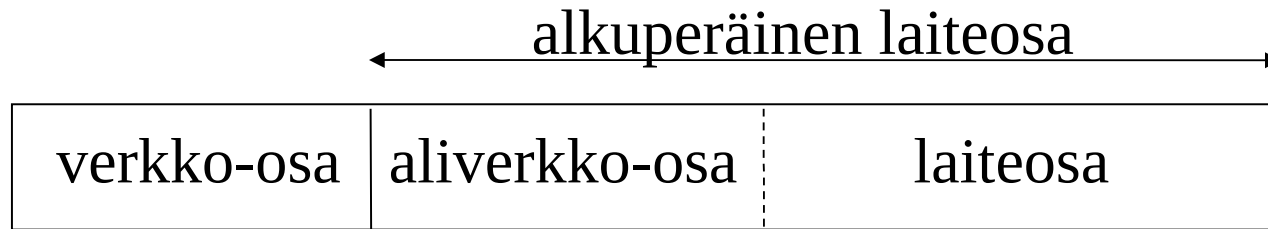
luokka	alku	verkko	laite	osoitteet
A	0	7 bittiä	24	1.0.0.0 - 126.255.255.255
B	10	14	16	128.0.0.0 - 191.255.255.255
C	110	21	8	192.0.0.0 - 223.255.255.255
D	1110	monilähetysryhmä		

- <http://www.xkcd.com/195/>

Nollien ja ykkösten merkitys

- tämä laite, 0.0.0.0
määrittelemättä
- laite tässä verkossa
- yleislähetys (tässä verkossa) 255.255.255.255
- verkkomaski 255.255.248.0
- loopback-osoite 127.0.0.1

Aliverkotus (RFC 940, 1985)



- Saman verkko-osoitteen käyttö useassa fyysisessä verkossa
- Osa laitetunnisteesta määrittääkin aliverkon
- Aliverkko-osan pituus voidaan määrittää verkkokohtaisesti

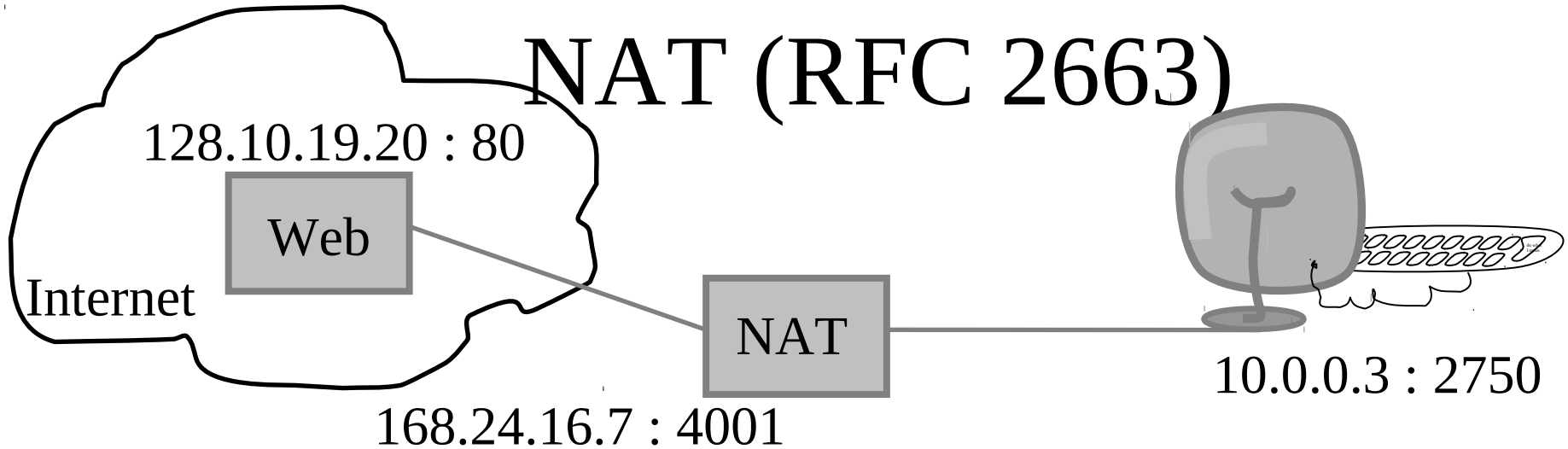
Luokaton osoitteistus (RFC 1518/1519, 1993)

- Classless InterDomain Routing (CIDR)
- Organisaation verkossa on useita verkkolohkoja
- Osoitelohkon koko voidaan valita vapaasti:
 - verkko-prefix / verkko-osan bittien määrä
 - esim2. 128.211.168.0/21, jossa verkkoa merkitsee 21 ensimmäistä bittiä osoitteesta, koneelle 11 viimeistä bittiä (verkossa tilaa 2048 koneelle)
 - esim 130.233.0.0/16 on tavallinen B-luokan osoite, Aallon:n verkko

NAT, DHCP, ICMP

Network Address Translation

NAT (RFC 2663)



- Piilottaa sisäverkon ulkopuolisilta, säästää osoitteita
 - reitittimellä tila kaikille yhteyksille
- Sisäverkossa voi käyttää yksityisiä osoitteita
 - 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12
- Voi aiheuttaa hankaluuksia sovelluksille (lisää 13.10.)

Dynamic Host Configuration Protocol DHCP (RFC2131)

- IP-osoitteen käyttölupa (lease) tietyksi ajaksi
 - automaattisesti (ekan kerran jälkeen aina sama osoite) tai dynaamisesti (joku osoite)
 - myös staattinen jako MAC-osoitteen perusteella mahdollinen
- Samalla muitakin asetustietoja, kuten nimipalvelimen osoite, oletusreitittimen osoite
 - Asiakas täyttää jo kyselyyn mahdollisimman paljon tietoja, ja jättää tyhjäksi (nollaksi), jos ei tiedä

DHCP-asiakkaan tilakone

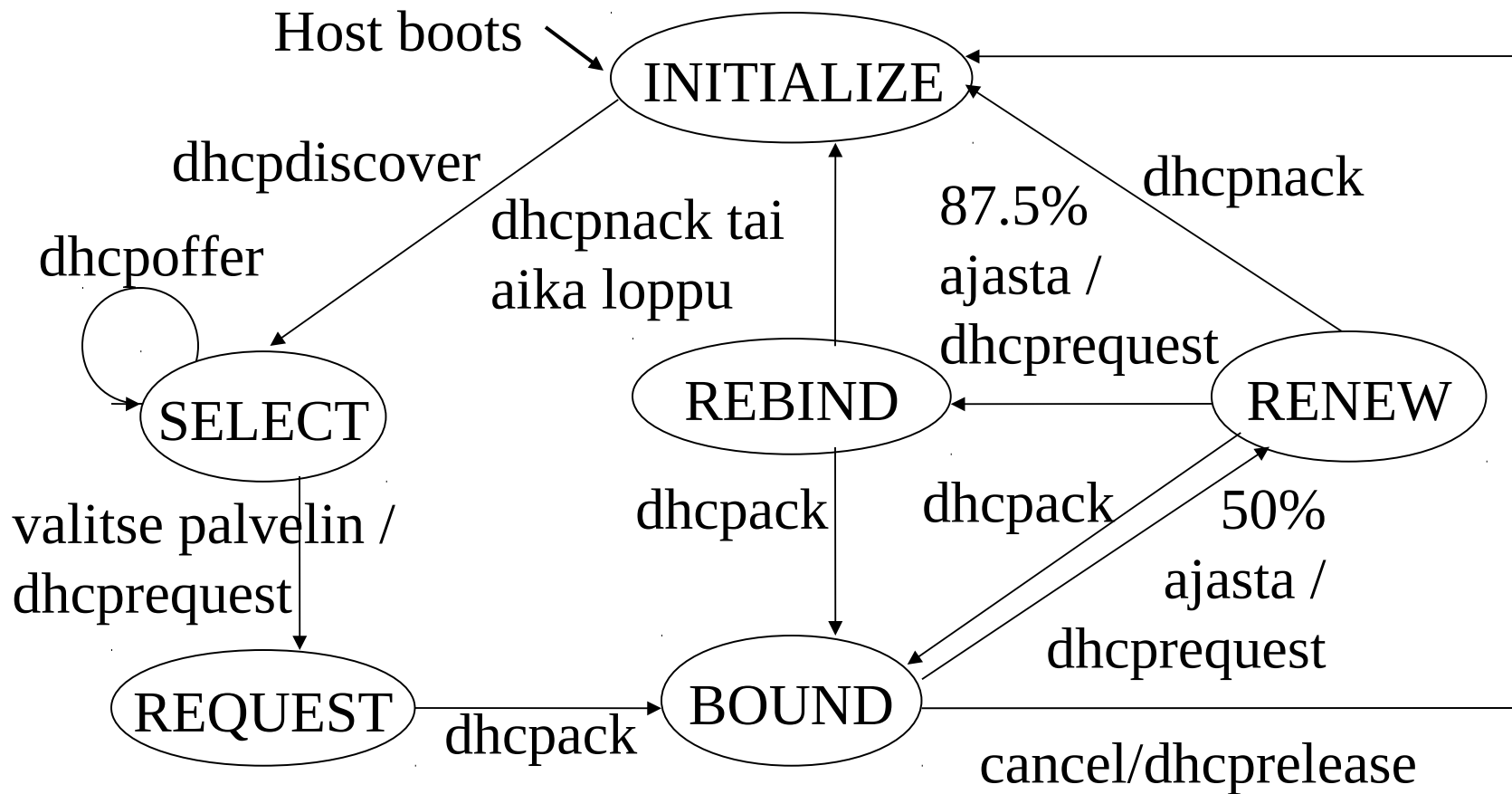


Fig. 22.3 in Comer

DHCP-viestit

0	8	16	24	31
OP	HTYPE	HLEN	HOPS	
XID				
SECS		FLAGS		
CLIENT IP ADDRESS				
YOUR IP ADDRESS				
SERVER IP ADDRESS				
RELAY AGENT IP ADDRESS				
CLIENT HARDWARE ADDRESS (16 oktetia)				
SERVER HOST NAME (64 oktetia)				
BOOT FILE (128 oktetia)				
optiot (vaihtuva)				

DHCP-viestit

- OP: 1 = kysely, 2 = vastaus
- HTYPE = linkkikerroksen verkon tyyppi
 - Ethernetille 1
- HLEN = linkkikerroksen osoitteen pituus
 - Ethernetille 6 (eli $6 \cdot 8 = 48$ bittiä)
- HOPS = asiakas asettaa nollaksi, käytetään kun välissä on välityspalvelin (relay agent)

DHCP-viestit

- XID = asiakkaan luoma tunniste
 - yhdistää kyselyt ja vastaukset
- SECS = sekunttia asiakkaan käynnistämisestä
- FLAGS = käytössä vain ensimmäinen bitti
 - 1 = vastaus lähetetään yleislähetyksenä (asiakkaalla ei vielä IP-osoitetta)
 - 0 = suoraan YOUR-kentän osoitteeseen yksilälähetyksenä

DHCP-viestit

- CLIENT-osoite, asiakkaan IP-osoite kun ARPia voidaan käyttää (bound, renew, rebinding-tilat), eli asiakas tietää osoitteensa
- YOUR-osoite, asiakkaan IP-osoite, palvelin lähettää asiakkaalle käynnistystyksen yhteydessä
- SERVER-osoite, jota pitäisi käyttää seuraavaksi (palvelin kertoo dhcpcoffer- ja -ack-tiloissa), myös jos asiakas haluaa tietyn palvelimen
- RELAY-osoite, jos välissä reititin/agentti

DHCP-viestit

- CLIENT HARDWARE = asiakkaan linkkikerroksen osoite
- Jos asiakas haluaa yhteyden tiettyyn palvelimeen, se täyttää joko palvelimen osoite -kentän tai kentän SERVER NAME = palvelimen dns-nimi

DHCP-viestit

- BOOT FILE = levyttömille koneille alustustiedoston sijainti
 - asiakas voi pyytää tiettyä, esim “unix”
 - palvelin joko antaa pyyntöä vastaavan sijainnin tai valitsee itse
 - asiakas hakee tiedoston esim TFTP:llä
- Optiot: type+length+value-tyylillä
 - esim. nimipalvelimen osoite
 - RFC 2132 sisältää mahdolliset optiot, lisäyksiä RFC3442, RFC3942, RFC4361, RFC4833, RFC5494

DHCP optiot

- aliverkon peite:

0	8	16	48
1	4	subnet mask	
- oletusreititin:

0	8	16	48	60	..	$n*4+16$
3	$n*4$	osoite1	osoite2	...	osoite n	

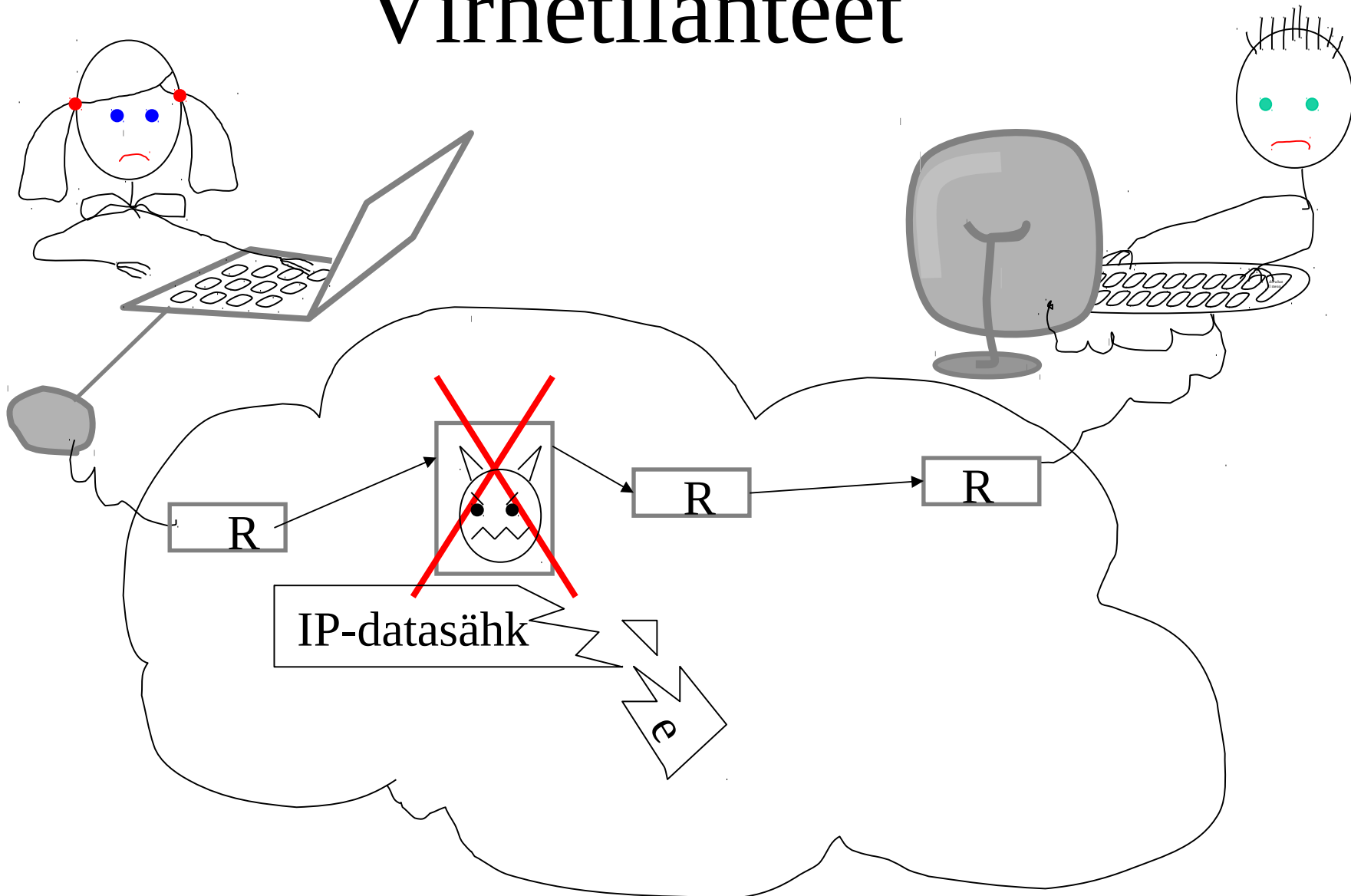
 - voi olla useita
 - preferenssijärjestyksessä
- nimipalvelin:

6	$n*4$	osoite1	osoite2	...	osoite n
---	-------	---------	---------	-----	----------

 - voi olla useita
 - preferenssijärjestyksessä

Virhetilanteet: ICMP

Virhetilanteet



Internet Control Message Protocol ICMP (RFC792)

- Ruuhkasta ilmoittaminen
- Uudelleenohjaus (tietoturvaongelma!)
- Elinajan raja saavutettu
- Parametriongelma
- Aliverkon peite
- Reitittimen etsiminen
- Polun pienimmän MTU:n löytäminen

Virhe- ja valvontaviestit

TYYPPI	KOODI	TARKASTUSSUMMA
Riippuu viestin tyypistä		
Ongelman aiheuttaneen paketin IP-otsikko ja 64 bittiä dataa		

- Internet Control Message Protocol (ICMP)
- Virhe- ja ohjaussanomat reitittimille ja tietokoneille
 - Ei virheiden korjausta, vain ilmoittaminen
- Lähetetään alkuperäiselle lähettäjälle

ICMP-viestejä

- Echo request ja echo reply (ping)

TYYPPI (8/0)	KOODI (0)	TARKASTUSSUMMA
TUNNISTE		JÄRJESTYSNUMERO
DATAA (ei välttämätön)...		

- Kohde tavoittamattomissa

TYYPPI (3)	KOODI (0)	TARKASTUSSUMMA
Käyttämätön (oltava 0)		
Ongelmapaketin IP-otsikko ja 64 bittiä dataa		

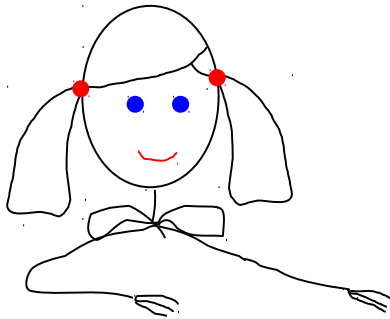
Lähteet

- RFC 791 Internet Protocol, 1981
- RFC 792 Internet Control Message Protocol, 1981
- RFC 796 Address Mappings, 1981
- RFC 950 Internet Standard Subnetting Procedure , 1985
- RFC 1518 An Architecture for IP Address Allocation with CIDR, 1993
- RFC 1519 Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strate, 1993
- RFC 2131 Dynamic Host Configuration Protocol, 1997
- RFC 2663 IP Network Address Translator (NAT) Terminology and Considerations, 1999
- RFC 3396 Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4), 2002
- RFC 4361 Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4), 2006

Lisää kursseja aiheesta

- T-110.5111 Computer networks II – advanced features (5 cr)
- S-38.2121 Reititys tietoliikenneverkoissa (4 op)
- S-38.3148 Simulation of Data Networks (5 cr)
- S-38.3180 Palvelunlaatu Internetissä (4 op)
- S-38.3184 Verkkoliikenteen mittaus ja analysointi L (5 op)

Ensi tiistaina: IPv6



SMTP	SIP	HTTP
SSH		IRC
TCP	UDP	SCTP
IP		
Ethernet	Token ring	
valokuitu	cat-5	

IP

Internet-protokolla

- Uusi versio Internet-protokollasta
- Miten IPv4 ja IPv6 toimivat samassa verkossa